Ex.7 IDS/IPS USING SNORT

AIM

To demonstrate how to use the "Snort" IDS/IPS tool to detect, prevent, and respond to network threats and attacks. Specifically, the experiment aims to:

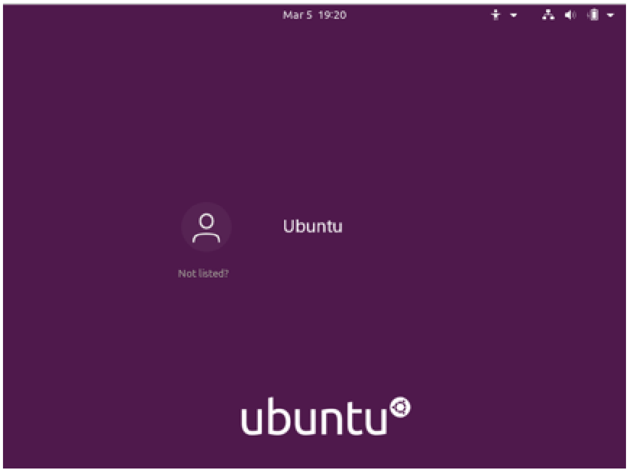
1. Install Ubuntu(Victim) and Kali Linux(Attacker) on separate VMs.
2. Install and configure Snort on Ubuntu to detect and prevent network intrusions.
3. Test Snort by pinging from Kali and verifying alerts generated by Snort.
4. Write new rules in Snort to allow any ICMP packet from an external device and FTP, & SSH packets from any device.
5. Test the new rules by sending ICMP, FTP, and SSH packets from Kali and verifying that Snort allows them (By alerts).

SOFTWARE REQUIRED: VM Virtual Box, Kali Linux OS, Ubuntu OS.

PROCEDURE:

1. Installation of Ubuntu.

Task 1-Installation and Setup of Ubuntu

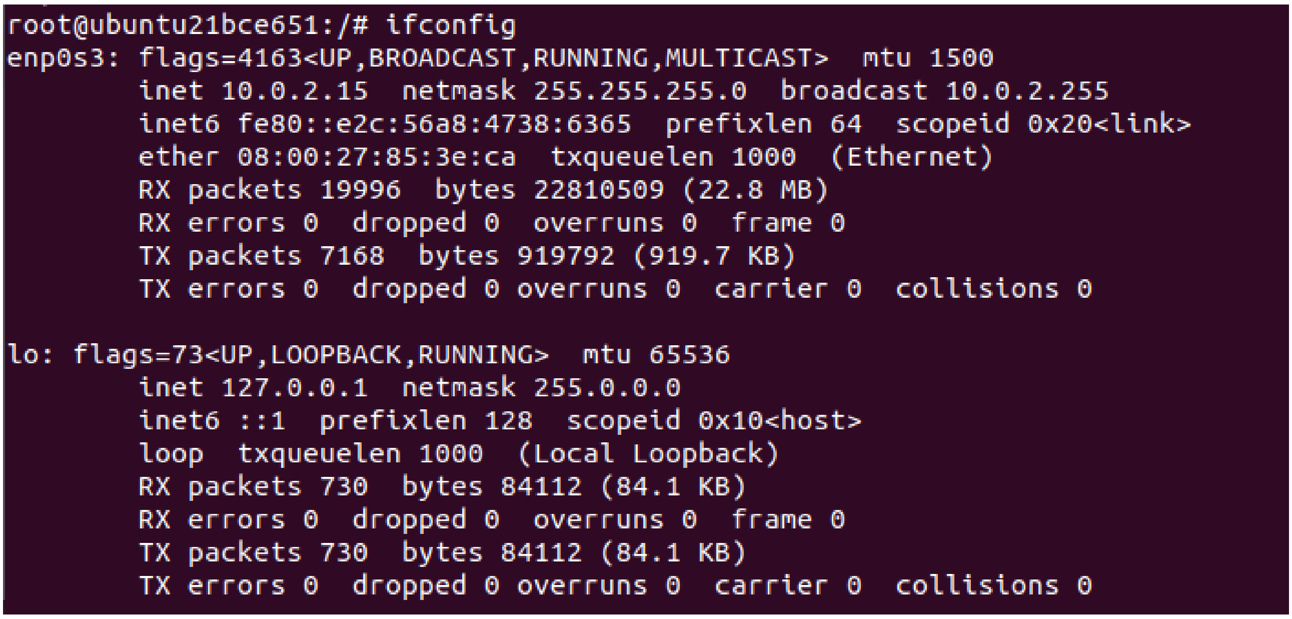
Output	Description
	Ubuntu ***".iso"***(Identical storage image of optical media is loaded into the VM Virtual box which then is used to create a new **".vdi"**(Virtual Disk Image) and then install ubuntu into the VM(follow the installation process). Once the OS is installed, start the VM and enter the previously set Username and password Username : "u_name" Password : "pwd" Have to be typed.

Task 2-Executing Snort Commands in Terminal to check Default Rules

2. Execute the commands stated below.

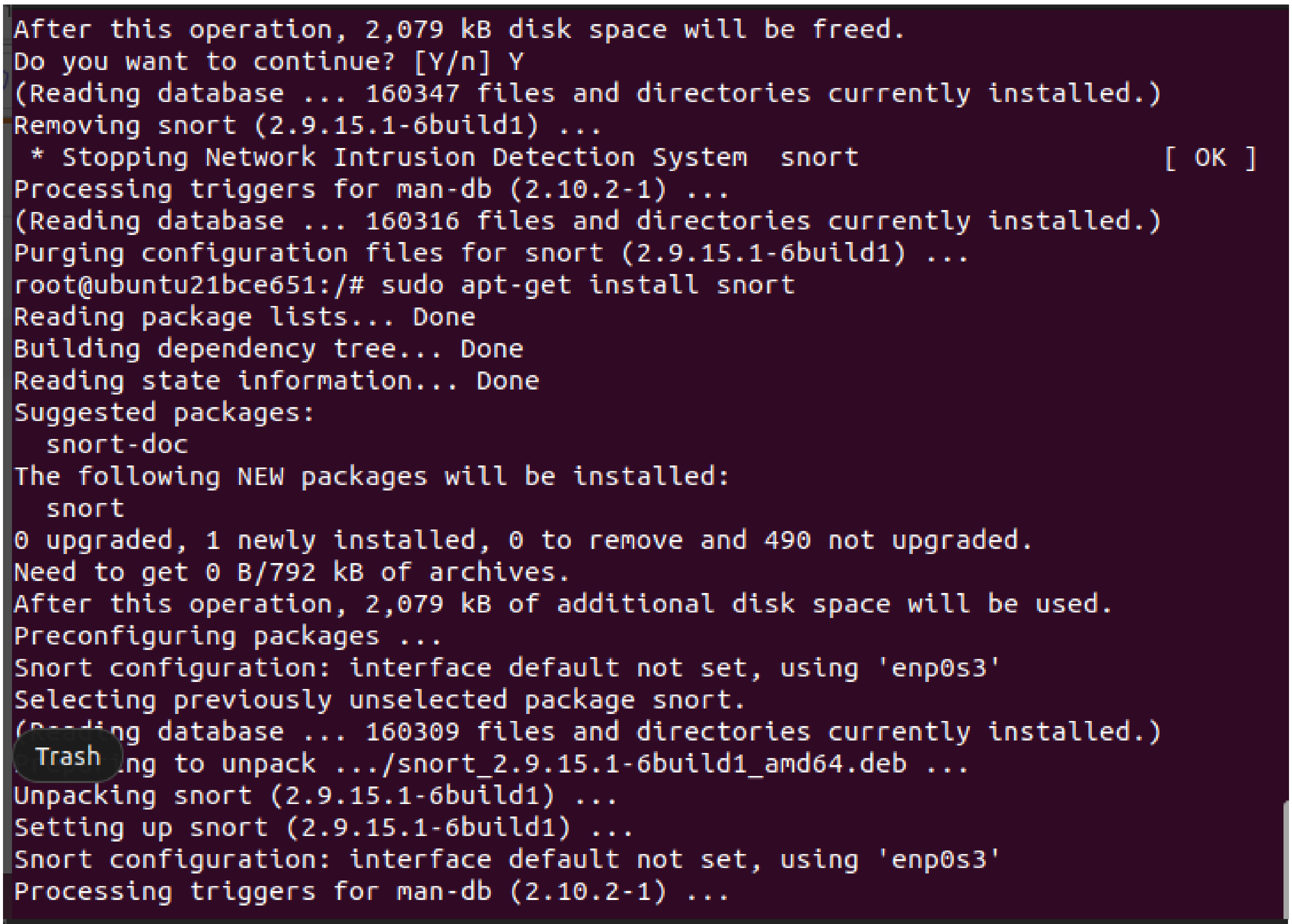
SNORT:

- Snort is an open-source network intrusion detection and prevention system (IDS/IPS) used tomonitor and analyse network traffic for security threats.
- It can detect various types of attacks such as port scans, buffer overflows, and stealth port scans.
- Snort provides real-time alerting capabilities when an attack is detected, enabling quick responses topotential security breaches.
- The system uses a rule-based language that allows users to create and customize rules for detectingspecific types of traffic or attacks.
- Snort can be used in a variety of network environments, including small businesses, largeenterprises, and service providers.
- The system can be deployed in a variety of configurations, including inline or passive, to meetdifferent security requirements.
- Snort is highly extensible and can be integrated with other security tools, such as firewalls andintrusion prevention systems, to create a comprehensive security solution.

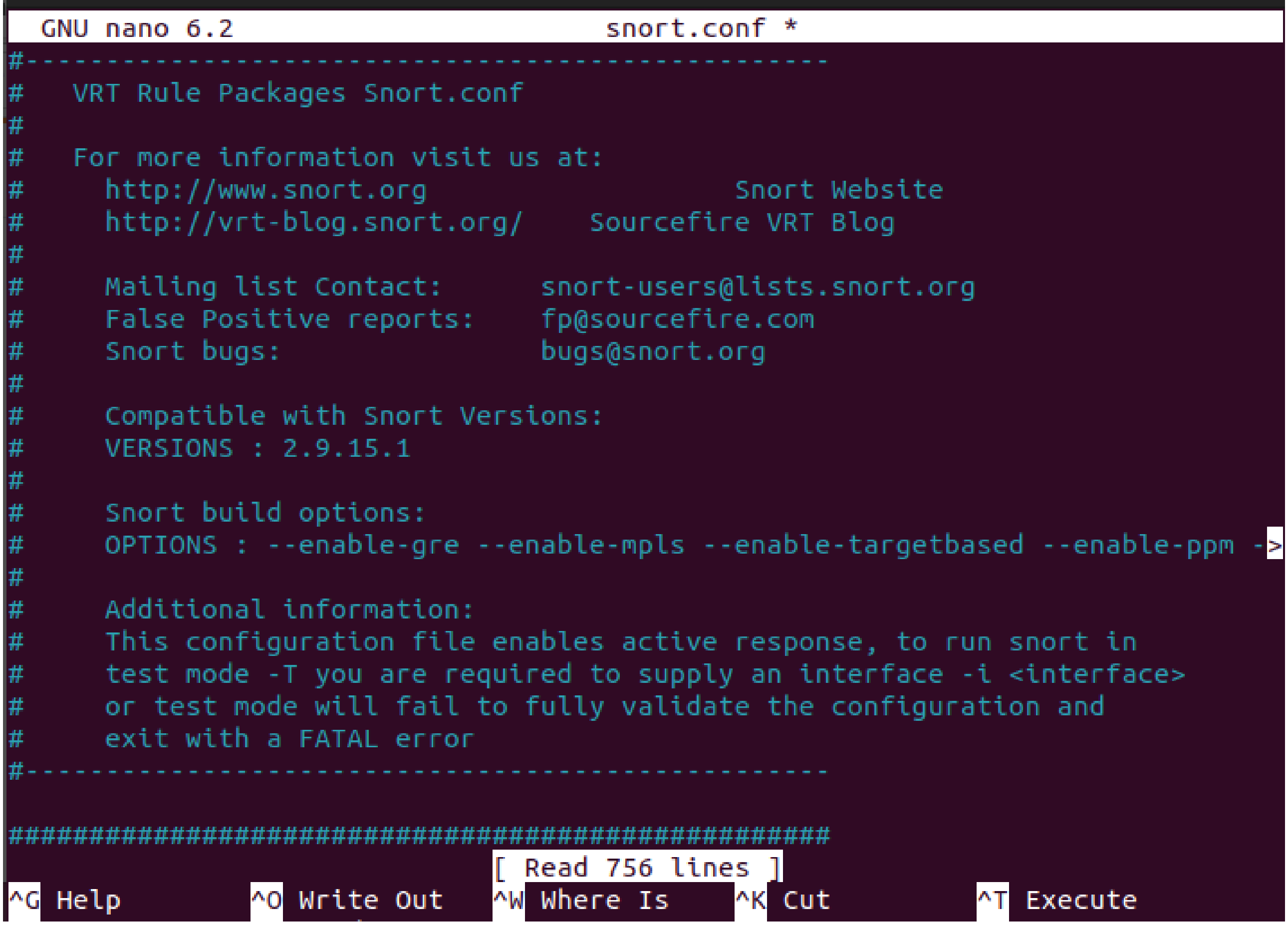


```
root@ubuntu21bce651:/# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::e2c:56a8:4738:6365  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:85:3e:ca  txqueuelen 1000  (Ethernet)
        RX packets 19996  bytes 22810509 (22.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7168  bytes 919792 (919.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 730  bytes 84112 (84.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 730  bytes 84112 (84.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



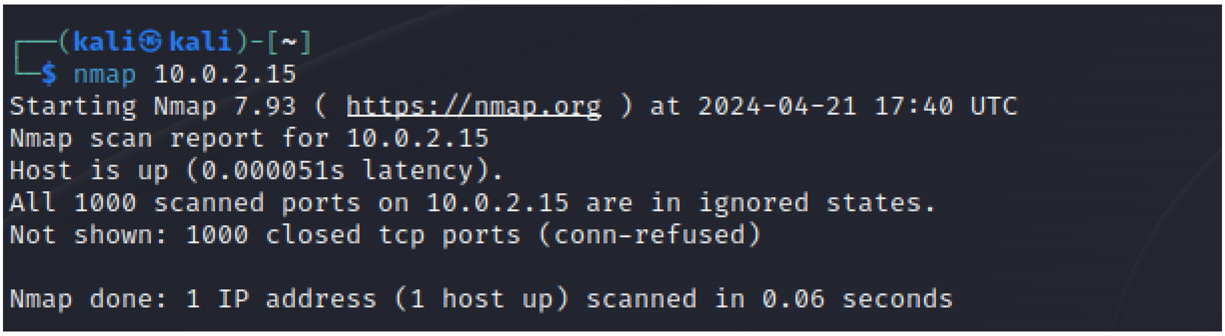
```
After this operation, 2,079 kB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 160347 files and directories currently installed.)
Removing snort (2.9.15.1-6build1) ...
 * Stopping Network Intrusion Detection System  snort                     [ OK ]
Processing triggers for man-db (2.10.2-1) ...
(Reading database ... 160316 files and directories currently installed.)
Purging configuration files for snort (2.9.15.1-6build1) ...
root@ubuntu21bce651:/# sudo apt-get install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  snort
0 upgraded, 1 newly installed, 0 to remove and 490 not upgraded.
Need to get 0 B/792 kB of archives.
After this operation, 2,079 kB of additional disk space will be used.
Preconfiguring packages ...
Snort configuration: interface default not set, using 'enp0s3'
Selecting previously unselected package snort.
(Reading database ... 160309 files and directories currently installed.)
Preparing to unpack .../snort_2.9.15.1-6build1_amd64.deb ...
Unpacking snort (2.9.15.1-6build1) ...
Setting up snort (2.9.15.1-6build1) ...
Snort configuration: interface default not set, using 'enp0s3'
Processing triggers for man-db (2.10.2-1) ...
```



```
  GNU nano 6.2                        snort.conf *
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#     http://www.snort.org                   Snort Website
#     http://vrt-blog.snort.org/    Sourcefire VRT Blog
#
#     Mailing list Contact:      snort-users@lists.snort.org
#     False Positive reports:    fp@sourcefire.com
#     Snort bugs:                bugs@snort.org
#
#     Compatible with Snort Versions:
#     VERSIONS : 2.9.15.1
#
#     Snort build options:
#     OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm ->
#
#     Additional information:
#     This configuration file enables active response, to run snort in
#     test mode -T you are required to supply an interface -i <interface>
#     or test mode will fail to fully validate the configuration and
#     exit with a FATAL error
#--------------------------------------------------

###################################################
                              [ Read 756 lines ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute
```

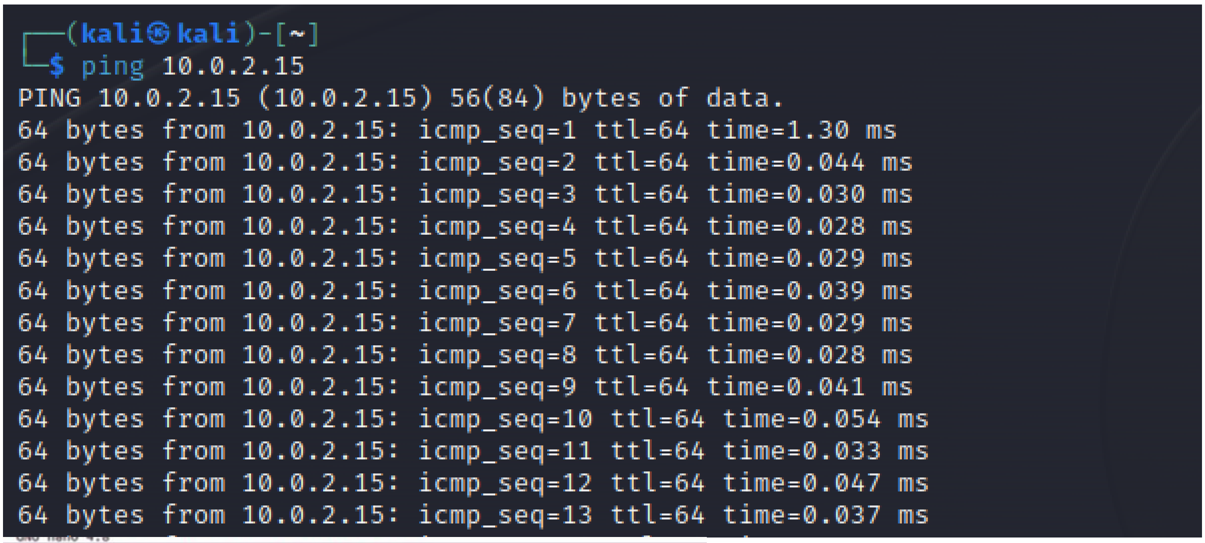
21BCE1651 – SANTHOSH KRISHNA R



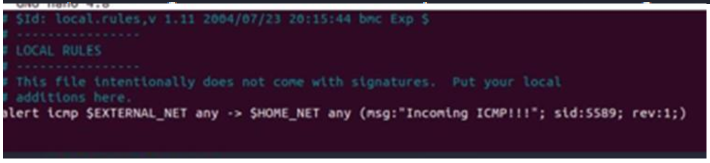
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-21 17:40 UTC
Nmap scan report for 10.0.2.15
Host is up (0.000051s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

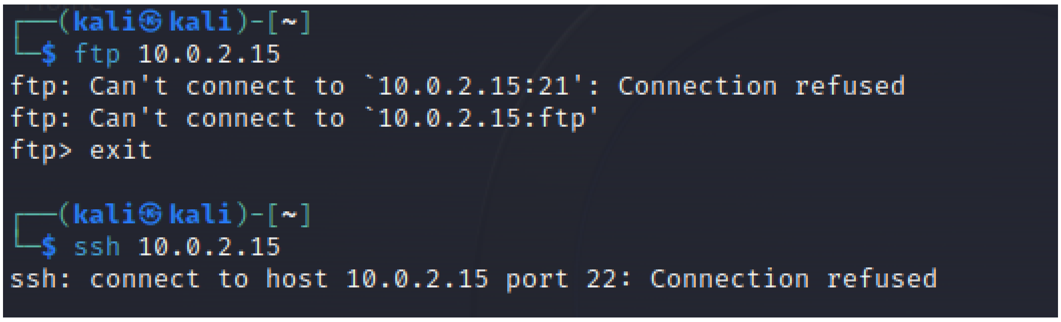
TASK – 3:



```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.044 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.030 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.028 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.029 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.039 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.029 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.028 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.041 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.054 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.033 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.047 ms
64 bytes from 10.0.2.15: icmp_seq=13 ttl=64 time=0.037 ms
```



```
GNU nano 4.8
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Incoming ICMP!!!"; sid:5589; rev:1;)
```



```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.15
ftp: Can't connect to `10.0.2.15:21': Connection refused
ftp: Can't connect to `10.0.2.15:ftp'
ftp> exit

┌──(kali㉿kali)-[~]
└─$ ssh 10.0.2.15
ssh: connect to host 10.0.2.15 port 22: Connection refused
```

21BCE1651 – SANTHOSH KRISHNA R